BOX PCT

IN THE UNITED STATES DESIGNATED OFFICE

OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

UNDER THE PATENT COOPERATION TREATY-CHAPTER II

PRELIMINARY AMENDMENT

APPLICANT(S): HARTWIG SCHWIER ET AL

ATTORNEY DOCKET NO. P01,0133

INTERNATIONAL APPLICATION NO: PCT/EP99/07329

INTERNATIONAL FILING DATE: 4 OCTOBER 1999

INVENTION: METHOD FOR OPERATING A COMPUTER WITH COPY PROTECTION FOR USER PROGRAMS

Assistant Commissioner for Patents

Washington, D.C. 20231

In the Specification:

Amend the specification as follows:

SPECIFICATION

TITLE

"METHOD FOR OPERATING A DATA PROCESSING SYSTEM WITH COPY PROTECTION FOR USER PROGRAMS"

Field of the Invention

The present invention is directed to a method for operating a data processing system with copy protection for user programs.

Description of the Related Art

The production of user programs requires considerable development time and specific know how; it is therefore relatively involved. User programs are often loaded onto storage media, for example on CDROMs, and supplied to the user in this condition. Such storage media are relatively inexpensive and are unrelated to the economic outlay that is incurred in the production of the user program. It is not only relatively easy to make legal backup copies of such storage media with traditional data processing systems, but pirated copies of these user programs can also be easily produced and handed over to further users for a certain price or distributed in some other way. The producer of the user programs thus suffers considerable damage.

Numerous copy protection methods have been developed in order to put an end to this practice. In a widespread copy protection method, a dongle is employed that is plugged onto a parallel interface, onto a serial interface or a USB bus of a data processing system. This dongle is supplied to the user together with the user program. The dongle as well as the user program contain the same copy protection identification in the form of alphanumerical characters. The presence of the dongle and, thus, of the copy protection information, is queried either at the program start or continuously during the program operation. When an attempt is made to operate the user program without the dongle, then the program is aborted.

When there are a great number of users who require different user programs, then a dongle is to be provided for each user. One storage medium per user must then be provided, the user programs intended for this user being contained thereon and then containing the same copy

protection identification as the respective dongle. When a user orders following user programs, then the following steps are required: producing a storage medium for this user; storing the user programs requested by the user; and providing the user programs with the copy protection identification of the dongle. Such a procedure is involved both for the user as well as for the producer of such user programs. US Patent No. 5,386,369 discloses a method based on dongles.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a method for operating a data processing system with copy protection for user programs that assures a dependable copy protection, works simply and can be realized with little outlay for producer and user.

According to the invention, a method for operating a data processing system with copy protection for user programs is provided, whereby a plurality of application programs as well as an installation program and a cryptoprogram are on hand on a storage medium, when processing the installation program on the data processing system, the user inputs a copy protection identification, a user identification that identifies the user and an encrypted product identification that identifies at least one user program,each user program contains a predetermined memory area into which the copy protection identification can be entered, the installation program compares the copy protection identification that has been input to a copy protection identification connected with the data processing system and, given coincidence, deciphers the encrypted product identification upon utilization of the user identification as a key, and identifies the user program selected in the product identification, the selected user program is loaded from the storage medium into a memory area of the data processing system, the cryptoprogram enters the copy protection identification into the predetermined memory area of the selected user program, and, before the running of the selected

user program, the copy protection identification contained in the predetermined memory area is compared to the copy protection identification connected with the data processing system, and the user program is run only given coincidence.

According to the present invention, a product identification and a user identification are communicated to the user. The product identification, preferably composed of alphanumerical characters, identifies -- in encrypted form -- the user program or, respectively, a plurality of user programs purchased by the user. Further, the user identification is likewise, for example, in the form of alphanumerical characters. This user identification serves as the key for the encryption and deciphering of the product identification. With the assistance of this product identification and the user identification, only those programs that are referenced in the product identification are enabled for the user. Accordingly, one storage medium, for example a CDROM, can contain all user programs of the manufacturer of the user programs. The customer or, respectively, user, however, can only access those user programs that he actually ordered and purchased and that can be enabled for him. The copy protection with the assistance of the copy protection identification is retained, i.e. the data processing system on which the user program is run is directly connected to a copy protection identification with the assistance of a hardware module. This user program can only be run on the specified data processing system when the user program also contains this copy protection identification; otherwise, operations are aborted. In this way, even the production of pirated copies and their forwarding to other users are worthless, since this other user does not possess the matching user identification, the matching product identification and the matching copy protection identification.

In one exemplary embodiment of the invention, the product identification also contains the copy protection identification, whereby this copy protection identification is also compared to the copy protection identification connected with the data processing system, and the running of the further program steps only continues given coincidence. Usually, the copy protection identification is assigned only once. Accordingly, a copy protection for the user programs themselves is still present even if the product identification is improperly handed over to another user.

An authentification between the installation program and the key program is preferably undertaken when calling the key program, which enters the copy protection identification in predetermined memory areas of the user program. In this way, a traditional, modular key program that usually runs on standard data processing systems can be employed. Nonetheless, a protection of the key program ensues due to the authentification between key program and installation program, and an adequate protection against misuse is established.

BRIEF DESCRIPTION OF THE DRAWINGS

An exemplary embodiment of the invention is explained below on the basis of the drawing

Figure 1 is a flowchart that shows critical steps of the inventive method;

Figure 2 is the flowchart when a new user orders one or more user programs; and

Figure 3 shows the executive sequence when an old user orders user programs.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows the critical steps of the method on the basis of a simple flowchart. The customer or user receives a plurality of user programs from the manufacturer of these user programs on a storage medium, for example a CDROM, according to the order. The user, for example, has only ordered a specific selection of user programs and only paid for these. Nonetheless, many other

user programs, which could be of use to the user in future and of which he can definitely make security copies, are on this storage medium. Further, the user receives a dongle from the manufacturer with a copy protection identification KI_D. This dongle must be plugged onto the parallel interface of the data processing system in order to be able to run the installation program and enable a proper operation of the user program, which has yet to be installed. Further, the user receives an alphanumerical user identification AI. This user identification serves later as the key for deciphering the product identification PI that is likewise given to the user. This product identification PI, for example, is likewise composed of alphanumerical characters and contains, on the one hand, the copy protection identification KI in encrypted form and, on he other hand, references a list of user programs that has been licensed to the user by the manufacturer as a result of the purchase.

In Figure 1, step 10, the installation program is loaded on the data processing system of the user and is started. The installation program contains a menu prompt and asks for the input of the copy protection identification KI given to the user, of the user identification AI and of the product identification PI (step 12). A check is carried out in step 14 to see whether the copy protection identification KI_E that has been input coincides with the copy protection identification KI_D contained in the dongle. When this is not the case, then a branch to the right is made is step 14 and the program execution is aborted.

An authentification of the installation program and of the key program ensues in a following step 16, i.e. a check is carried out to see whether the installation program originally contained on the storage medium and the key program are allowed to mutually call one another. The authentification ensues, for example, according to the challenge-response principle, which represents a standard

method for the protection of programs. When the authentification proceeds successfully, a branch is made to step 18; otherwise, a program abort follows. The sequence of the steps can also be such that step 16 is run first and step 14 thereafter.

In step 18, the encrypted product identification PI that, for example, has been encrypted according to the high-compression Huffmann-Baum method is deciphered. The user identification AT given to the user is used as the key in this deciphering. The result of the deciphering step 18 is that the copy protection identification KI_{PI} and the list of user programs wanted by the user is obtained.

In the following step 20, this list of the user programs is checked for plausibility, i.e. a determination can be made as to whether the correct user programs are present. Additionally, a checksum check of the list ensues in order to prevent au unauthorized expansion of the license on the part of the customer (signature function).

In step 12, the copy protection identification KI_{PI} contained in the product identification PI is compared to the copy protection identification KI_D of the dongle of the data processing system. One proceeds to the next step 24 given coincidence. Otherwise, the program execution is aborted. In step 24, the user can again make a selection from the list of user programs he requested, for example select those user programs that are minimally needed for handling a specific job.

In the following step 26, datafiles that are needed for the user programs and their running are established in the data processing system. The key program enters the copy protection identification KI into predetermined memory areas for the selected user programs. The installation of the user programs has thus been ended in step 28.

When running the user programs, the copy protection identification KI contained in the respective user program is compared to the copy protection identification KI_D of the dongle, as is traditional. The user program is run by the data processing system only given coincidence.

As can be seen, advantages derive both at the producer side as well as at the user side. The producer can store a plurality of user programs on the available storage medium, for example all user programs that are made available to users. Thus, the producer need not write a new storage medium dependent on the order of a specific user; rather, a limitation can be made to a single storage medium or to a few storage media. The outlay for offering storage media is lowered in this way. A similar advantage derives on the part of the user. The user, upon delivery, receives a plurality of user programs from which the user can enable precisely those that the user had ordered and purchased. When the user would like to purchase another user program at a later time, then the only thing required is the enable of this user program, which already exists, by handing over a new product identification PI. The user identification AI can remain the same. The installation itself is simple and only requires a short time. The delivery of a new dongle or of a new storage medium is not required in many cases.

The executive sequence shown in Figure 1 can be modified in many respects. For example, the user programs can also be kept on hand in a central storage medium that the user can access with the Internet. Another modification provides that, after a number of user programs have been offered to the user, these are only partly enabled and activated for demonstration purposes of user programs that were not ordered. The user can then see the advantage of such further user programs and potentially order them, whereby a new storage medium for example a new CDROM, need not be sent.

On the basis of a flowchart, Figure 2 shows the advantages of the method when a new user, who does not yet have access to the storage medium with the user programs, orders user programs (block 30) and is licensed therefor by the producer. The producer defines the user data, i.e. a user identification AI and a product identification PI are produced; further, a dongle with a copy protection identification KI is offered (block 32). The data are stored (block 34) in a data bank. The user is provided with the user data, i.e. the dongle, the copy protection identification KI, the product identification PI and the user identification AI. Further, the user is provided with a CDROM on which a plurality of user programs is stored (block 36). The installation of the user programs selected by the user ensues at the user according to the executive sequence steps according to Figure 1 (block 38).

Figure 3 shows the executive sequence when an old user, who already has a CDROM with the plurality of user programs, a dongle, a copy protection identification KI and a user identification AI, orders user programs (block 40). The producer defines the user data (block 42), i.e. the product identification PI (block 44). The user identification AI can remain the same. The corresponding data are stored in the data bank (block 46). The user data are given to the user (block 48). The installation of the user programs ensues according to the method steps (block 50) indicated in Figure 1.

Although other modifications and changes may be suggested by those skilled in the art, it is the intention of the inventors to embody within the patent warranted hereon all changes and modifications as reasonably and properly come within the scope of their contribution to the art.